Claims

What is claimed is:

1. Apparatus for providing decision support to an analyst in accordance with an event management system which manages a network with one or more computing devices, the apparatus comprising:

at least one processor operative to perform: (i) an automated analysis of data representing past events associated with the network of computing devices being managed by the event management system, the automated analysis comprising generation of one or more visualizations of one or more portions of the past event data and discovery of one or more patterns in the past event data; and (ii) automated rule management comprising construction and validation of one or more rules formed in accordance with the automated analysis of the past event data; and

memory, coupled to the at least one processor, which stores at least a portion of results associated with the automated event analysis and rule management operations.

2. The apparatus of claim 1, wherein the past event data is obtained from an event database and the one or more rules are provided to a rule database, the event database and the rule database being associated with an execution system of the event management system.

3. The apparatus of claim 2, wherein generation of the one or more visualizations of the one or more portions of the past event data further comprises:

selecting a subset of the past event data from the event database;

generating a visualization of the subset of past event data using a visualization tool;

the analyst reviewing the visualization to determine whether there are any groupings of events that are of interest presented therein; and

performing an appropriate action when an event grouping of interest is found.

4. The apparatus of claim 2, wherein discovery of the one or more patterns in the past event data further comprises:

selecting a subset of the past event data from the event database;

mining the subset of the past event data to discover the one or more patterns using a mining tool;

generating a visualization of the one or more patterns using a visualization tool;

the analyst reviewing the visualization to determine whether there are any patterns of interest presented therein; and

performing an appropriate action when a pattern of interest is found.

5. The apparatus of claim 2, wherein validation of the one or more rules further comprises:

selecting a subset of the past event data from the event database;

finding one or more instances of patterns expressed in terms of left-hand sides of rules;

generating a visualization of the one or more pattern instances using a visualization tool;

analyzing the left-hand sides of rules using a rule validation tool;

displaying results of the analysis operation;

the analyst assessing analysis results; and

marking the rules as one of validated and not validated based on the assessment by the analyst.

6. The apparatus of claim 2, wherein construction of the one or more rules further comprises:

selecting a subset of the past event data from the event database;

mining the subset of the past event data to discover the one or more patterns using a mining tool;

assessing significance of the one or more patterns using a visualization tool;

constructing the one or more rules from a selected subset of the one or more patterns using a rule construction tool; and

writing the one or more rules in the rule database.

7. A computer-based method of providing decision support to an analyst in accordance with an event management system which manages a network with one or more computing devices, the method comprising the steps of:

automatically analyzing data representing past events associated with the network of computing devices being managed by the event management system, the automated analysis comprising generation of one or more visualizations of one or more portions of the past event data and discovery of one or more patterns in the past event data; and

automatically managing rules, the automated rule management comprising construction and validation of one or more rules formed in accordance with the automated analysis of the past event data.

8. The method of claim 7, wherein the past event data is obtained from an event database and the one or more rules are provided to a rule database, the event database and the rule database being associated with an execution system of the event management system.

9. The method of claim 7, wherein generation of the one or more visualizations of the one or more portions of the past event data further comprises:

selecting a subset of the past event data from the event database;

generating a visualization of the subset of past event data using a visualization tool;

the analyst reviewing the visualization to determine whether there are any groupings of events that are of interest presented therein; and

performing an appropriate action when an event grouping of interest is found.

10. The method of claim 7, wherein discovery of the one or more patterns in the past event data further comprises:

selecting a subset of the past event data from the event database;

mining the subset of the past event data to discover the one or more patterns using a mining tool;

generating a visualization of the one or more patterns using a visualization tool;

the analyst reviewing the visualization to determine whether there are any patterns of interest presented therein; and

performing an appropriate action when a pattern of interest is found.

11. The method of claim 7, wherein validation of the one or more rules further comprises:

selecting a subset of the past event data from the event database;

finding one or more instances of patterns expressed in terms of left-hand sides of rules;

generating a visualization of the one or more pattern instances using a visualization tool;

analyzing the left-hand sides of rules using a rule validation tool;

displaying results of the analysis operation;

the analyst assessing analysis results; and

marking the rules as one of validated and not validated based on the assessment by the analyst.

12. The method of claim 7, wherein construction of the one or more rules further comprises:

selecting a subset of the past event data from the event database;

mining the subset of the past event data to discover the one or more patterns using a mining tool;

assessing significance of the one or more patterns using a visualization tool;

constructing the one or more rules from a selected subset of the one or more patterns using a rule construction tool; and

writing the one or more rules in the rule database.

13. An article of manufacture for providing decision support to an analyst in accordance with an event management system which manages a network with one or more computing devices, the article comprising a machine readable medium containing one or more programs which when executed implement the steps of:

automatically analyzing data representing past events associated with the network of computing devices being managed by the event management system, the automated analysis comprising generation of one or more visualizations of one or more portions of the past event data and discovery of one or more patterns in the past event data; and

automatically managing rules, the automated rule management comprising construction and validation of one or more rules formed in accordance with the automated analysis of the past event data.

14. The article of claim 13, wherein the past event data is obtained from an event database and the one or more rules are provided to a rule database, the event database and the rule database being associated with an execution system of the event management system.

15. Apparatus for providing decision support to an analyst in accordance with an event management system which manages a network with one or more computing devices, the apparatus comprising:

first processing means for performing an automated analysis of data representing past events associated with the network of computing devices being managed by the event management system, the automated analysis comprising generation of one or more visualizations of one or more portions of the past event data and discovery of one or more patterns in the past event data;

second processing means for performing automated rule management comprising construction and validation of one or more rules formed in accordance with the automated analysis of the past event data; and

memory means, coupled to the first and second processing means, for storing at least a portion of results associated with the automated event analysis and rule management operations.

16. The apparatus of claim 15, wherein the past event data is obtained from an event database and the one or more rules are provided to a rule database, the event database and the rule database being associated with an execution system of the event management system.

17. An event management decision support system for providing decision support to an analyst in accordance with an event management system which manages a network with one or more computing devices, the system comprising:

one or more data analysis tools for automatically analyzing, in an off-line condition, data representing events associated with the network of computing devices being managed by the event management system, the automated analysis comprising generation of one or more visualizations of one or more portions of the event data and discovery of one or more patterns in the event data; and

one or more rule management tools for automatically managing rules in an off-line condition, the automated rule management comprising construction and validation of one or more rules formed in accordance with the automated analysis of the event data.

18. The system of claim 17, wherein the event data is obtained from an event database and the one or more rules are provided to a rule database, the event database and the rule database being associated with an execution system of the event management system.